CLAIMS

Please amend the claims as follows and cancel claims 1-8, 10-17 and 21-32 without prejudice.

Claims 1-8 (Canceled)

9. (Currently amended) A method for performing an initial handshake during secure communications in a computer network comprising:

coupling a client to a web server;

generating a ~~Rivest-Shamir-Adleman ("RSA")~~ algorithm public / private key pair at the web server, wherein the ~~RSA~~ public key is a product of two distinct prime numbers and the private key is a function of two randomly generated numbers such that $<r_1, r_2>$ satisfies $d=r_1 \bmod (p-1)$ and $d=r_2 \bmod (q-1)$, wherein each random number has a number of bits greater than or equal to 160 bits and less than a number of bits of the ~~RSA~~public key;

sending a client hello message to the web server requesting a secure network connection;

responding to the client with a server hello message containing the ~~RSA~~ public key;

encrypting a random string R at the client using the ~~RSA~~ public key, wherein the resulting cipher-text C includes R;

sending the encrypted cipher-text message to the web server;

separating cipher-text moduli of the two distinct prime numbers, wherein cipher-text moduli refers to a mod(p,q);

decrypting the moduli of the two distinct prime numbers individually using the two random numbers, wherein the results are combined using the Chinese Remainder Theorem, wherein computational ~~efficiency is improved~~time is decreased; [[and]]

establishing a common session key between the web server and the client using R;

combining individually encrypted messages into a set of encrypted messages wherein each encrypted message possesses a public key comprising:

an encryption exponent;

determining a root node of a binary tree containing leaf nodes

corresponding to each encryption exponent using a plurality of separate parallel batch trees, wherein the root node of each tree is found and combined to determine the final answer;

minimizing a disparity between sizes of the encryption exponents of the within the set;

using simultaneous multiple exponentiation such that the encryption exponents are combined to reduce the number of exponentiations;

calculating a product of the encrypted messages;

extracting at least one root from the product of the encrypted messages; and

decrypting the encrypted messages by expressing the at least one root as at least one promise and evaluating the at least one promise at the leaf nodes, and multiplying an inversion of a total product of the leaf nodes with a partial product of the leaf nodes forming an inversion of the leaf node, producing a reduced number of modular inversions wherein a length of time of the decryption is decreased.

Claims 10-17 (Canceled)

18. (Currently amended) ~~The method of claim 17, further~~ A method for decryption of secure network communications, comprising:

generating a public/private key pair at a web server, wherein <N,e> represents the public key that is mathematically related to two distinct prime numbers;

keeping a size of N constant while reducing a size of the two distinct prime numbers by calculating N from a product of a first distinct prime number raised to the first power and a second distinct prime number wherein the first power is greater than one;

using the public key by a client to encrypt a plain-text message R to form a cipher-text message C;

decrypting the cipher-text C at the web server by using the private key d to determine the plain-text message R by finding R'_1 and R'_2, wherein the private key is a function of two randomly generated numbers such that $<r_1, r_2>$ satisfies

$d=r_1 \bmod (p-1)$ and $d=r_2 \bmod (q-1)$, and wherein an additional R''_1 is constructed by using one of the two distinct prime numbers raised to a power greater than one, wherein a length of time of the decryption is decreased in response to the reduced size of the two distinct prime numbers; and

computing the plain-text message using the Chinese Remainder Theorem;

combining individually encrypted network security protection handshake messages into a set of encrypted messages wherein each encrypted message is derived using a public key containing an encryption exponent;

determining a root node of a binary tree comprising leaf nodes corresponding to each encrypted messages encryption exponent by using a plurality of separate, parallel batch trees finding the root node of each tree and combining the final answers;

minimizing the disparity between the sizes of the encryption exponents of the public keys within the set;

using simultaneous multiple exponentiation such that the encryption exponents are combined to reduce the number of exponentiations;

calculating a product of the encrypted messages;

extracting at least one root from the product of the encrypted messages; and

decrypting the encrypted messages by expressing the at least one root as at least one promise and evaluating the at least one promise at the leaf nodes, and multiplying an inversion of a total product of the leaf nodes with a partial

product of the leaf nodes forming an inversion of the leaf node wherein the decryption is increased by reducing the number of modular inversions.

19. (Currently amended) ~~The method of claim 17,~~A method for decryption of secure network communications, comprising:

generating a public/private key pair at a web server, wherein <N,e> represents the public key that is mathematically related to two distinct prime numbers;

keeping a size of N constant while reducing a size of the two distinct prime numbers by calculating N from a product of a first distinct prime number raised to the first power and a second distinct prime number wherein the first power is greater than one;

using the public key by a client to encrypt a plain-text message R to form a cipher-text message C;

decrypting the cipher-text C at the web server by using the private key d to determine the plain-text message R by finding R'_1 and R'_2, wherein the private key is a function of two randomly generated numbers such that $<r_1, r_2>$ satisfies $d=r_1 \bmod (p-1)$ and $d=r_2 \bmod (q-1)$, and wherein an additional R''_1 is constructed by using one of the two distinct prime numbers raised to a power greater than one, wherein a length of time of the decryption is decreased in response to the reduced size of the two distinct prime numbers, and wherein the k-bit values r_1, r_2 are related to the n-bit primes by the greatest common divisor of $(r_1, p-1) = 1$, $(r_2, q-1) = 1$, $r_1 = r_2 \bmod w$ respectively such that $d = r_1 \bmod p-1$, $d = r_2 \bmod q-1$, and w is equal to the greatest common divisor of (p-1, q-1); and

computing the plain-text message using the Chinese Remainder Theorem.

20. (Currently amended) ~~The method of claim 17,~~A method for decryption of secure network communications, comprising:

generating a public/private key pair at a web server, wherein <N,e> represents the public key that is mathematically related to two distinct prime numbers;

keeping a size of N constant while reducing a size of the two distinct prime numbers by calculating N from a product of a first distinct prime number raised to the first power and a second distinct prime number wherein the first power is greater than one;

using the public key by a client to encrypt a plain-text message R to form a cipher-text message C;

decrypting the cipher-text C at the web server by using the private key d to determine the plain-text message R by finding R'_1 and R'_2, wherein the private key is a function of two randomly generated numbers such that $<r_1, r_2>$ satisfies $d=r_1 \bmod (p-1)$ and $d=r_2 \bmod (q-1)$, and wherein an additional R''_1 is constructed by using one of the two distinct prime numbers raised to a power greater than one, wherein a length of time of the decryption is decreased in response to the reduced size of the two distinct prime numbers, and wherein decrypting includes[[:]] computing R_1', R''_1, and R_2' as expressed by the relationships $R'_1 = C^{r1} \bmod p$, $R'_2 = C^{r2} \bmod q$, and $R_1'' = R_1' - \frac{(R_1')^e - C}{e(R_1')^{e-1}} (\bmod p^2)$; and

computing the plain-text message using the Chinese Remainder Theorem.

Claims 21-32 (Canceled).